Many of the following exercises require a computer and PARI/GP.
Here are the links to some programs which you can paste into PARI/GP and use.

Trial division: `http://www.mat.uniroma2.it/~geatti/ERBIL2024/naif.txt`

Pollard ρ: `http://www.mat.uniroma2.it/~geatti/ERBIL2024/pollard.txt`

Pollard $p-1$: `http://www.mat.uniroma2.it/~geatti/ERBIL2024/pminus.txt`

Miller-Rabin test: `http://www.mat.uniroma2.it/~geatti/ERBIL2024/mrtest.txt`

Naif versus Pollard: `http://www.mat.uniroma2.it/~geatti/ERBIL2024/PollardVersusNaif.txt`

Trial division factoring algorithm

1. Use the “trial division” algorithm to factor

$$n = 10069889000883108903279549 77.$$

2. On the base of the estimates of the previous exercise, exhibit integers whose factorisation with trial division requires one month, one year, 10 years.

Pollard ρ

3. Let n be a composite integer of 200 digits. After 10000 iterations the Pollard ρ algorithm did not find any factors. What can we conclude about the size of the prime factors?

4. Let n be a composite integer of 200 digits, and let $B = 10000$. After how many unsuccessful iterations of the Pollard ρ algorithm we can conclude that probably n has no factor $\leq B$?

5. Factor completely the integers (you may have to apply pollard several times):

   $n_1 = 1077471755063687$

   $n_2 = 10687643000000395442791$

   $n_3 = 1000587688300000000000000000000000008574912503519308271870011$

   $n_4 = 10760671013000000000000000000000000000000000000000000000000000000000000000000000000000$
   $000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000$
   $00824221115473495059110442157250483.$

   $n_5 = 10000076067099100000000000000000000000000000000000000000000000000000000000000000000000$
   $000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000$
   $007659628141113788389728281238427868281.$